Part One

The Case for Action

(Intentionally Left Blank)

Chapter One

Acting Now to Protect the Future

"We are at the dawn of a new century. Now is the moment to be farsighted as we chart a path into the new millennium."

— President William J. Clinton, "A National Security Strategy for a New Century," May 1997

Life is good in America because things work. When we flip the switch, the lights come on. When we turn the tap, clean water flows. When we pick up the phone, our call goes through. We are able to assume that things will work because our *infrastructures* are highly developed and highly effective. By *infrastructure* we mean more than just a collection of individual companies engaged in related activities; we mean a network of independent, mostly privately-owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services.

Businesses, too, depend on infrastructures. Private companies are able to guarantee on-time performance because our infrastructures permit low cost transport and instantaneous tracking of shipments. Managers take for granted that the goods and services essential to their operations will be there when needed.

Reliable and secure infrastructures are thus the foundation for creating the wealth of our nation and our quality of life as a people. They are fundamental to development and projection of the military power that enables our diplomacy to be effective. They make it possible for us to enjoy our inalienable rights and take advantage of the freedoms on which our nation was founded. Certain of our infrastructures are so vital that their incapacity or destruction would have a debilitating impact on our defense and economic security.

The ***transportation*** infrastructure moves goods and people within and beyond our borders, and makes it possible for the United States to play a leading role in the global economy.

The ***oil and gas production and storage*** infrastructure fuels transportation services, manufacturing operations, and home utilities.

The ***water supply*** infrastructure assures a steady flow of water for agriculture, industry (including various manufacturing processes, power generation, and cooling), business, firefighting, and our homes.

The ***emergency services*** infrastructure in communities across the country responds to our urgent police, fire, and medical needs, saving lives and preserving property.

The ***government services*** infrastructure consists of federal, state, and local agencies that provide essential services to the public, promoting the general welfare.

The ***banking and finance*** infrastructure manages trillions of dollars, from deposit of our individual paychecks to the transfer of huge amounts in support of major global enterprises.

The ***electrical power*** infrastructure consists of generation, transmission, and distribution systems that are essential to all other infrastructures and every aspect of our economy. Without electricity, our factories would cease production, our televisions would fade to black, and our radios would fall silent (even a battery-powered receiver depends on an electric-powered transmitter). Our street intersections would suddenly be dangerous. Our homes and businesses would go dark. Our computers and our telecommunications would no longer operate.

The ***telecommunications*** infrastructure has been revolutionized by advances in information technology in the past two decades to form an ***information and communications*** infrastructure, consisting of the Public Telecommunications Network (PTN), the Internet, and the many millions of computers in home, commercial, academic, and government use. Taking advantage of the speed, efficiency and effectiveness of computers and digital communications, all the critical infrastructures are increasingly connected to networks, particularly the Internet. Thus, they are connected to one another. Networking enables the electronic transfer of funds, the distribution of electrical power, and the control of gas and oil pipeline systems. Networking is essential to a service economy as well as to competitive manufacturing and efficient delivery of raw materials and finished goods. The information and communications infrastructure is basic to responsive emergency services. It is the backbone of our military command and control system. And it is becoming the core of our educational system.

Disruption of any infrastructure is always inconvenient and can be costly and even life threatening. Major disruptions could lead to major losses and affect national security, the economy, and the public good. Mutual dependence and the interconnectedness made possible by the information and communications infrastructure lead to the possibility that our infrastructures may be vulnerable in ways they never have been before. Intentional exploitation of these new vulnerabilities could have severe consequences for our economy, security, and way of life.

Technologies and techniques that have fueled major improvements in the performance of our infrastructures can also be used to disrupt them. The United States, where close to half of all computer capacity and 60 percent of Internet assets reside, is at once the world's most advanced and most dependent user of information technology. More than any other country, we rely on a set of increasingly accessible and technologically reliable infrastructures, which in turn have a growing collective dependence on domestic and global networks. This provides great opportunity, but it also presents new vulnerabilities that can be exploited. It heightens risk of cascading technological failure, and therefore of cascading disruption in the flow of essential goods and services. Computerized interaction within and among infrastructures has become so complex that it may be possible to do harm in ways we cannot yet conceive.

The threat is real enough. The terrorist bombings of the US World Trade Center, the federal building in Oklahoma City, and the El Khobar quarters in Saudi Arabia have demonstrated all too well the malevolent intent of some parties toward the United States. Skilled computer operators have demonstrated their ability to gain access to networks without authorization. Some do it for the thrill or the notoriety. Some do it for financial gain. Some do it to further a cause. Whatever the motivation, their success in entering networks to alter data, extract financial or proprietary information, or introduce viruses demonstrates that it can be done and gives rise to concerns that, in the future, some party wishing to do serious damage to the United States will do so by the same means.

Real vulnerabilities also exist. Infrastructures have always been subject to local or regional outages resulting from earthquakes, storms, and floods. Their owners and operators, in cooperation with local, state, and federal emergency services, have demonstrated their capacity to restore services efficiently. Physical vulnerabilities to man-made threats, such as arson and bombs, are likewise not new. But physical vulnerabilities take on added significance as new capabilities to exploit them emerge, including chemical, biological, and even nuclear weapons. As weapons of mass destruction proliferate, the likelihood of their use by terrorists increases.

Terrorist attacks have typically been against single targets—individuals, buildings, or institutions. Today, more sophisticated physical attacks may also exploit the emerging vulnerabilities associated with the complexity and interconnectedness of our infrastructures. Bombs—even homemade ones—have always been able to damage a pipeline, electrical power transformer, telecommunications switching station, or microwave relay antenna. In the networked world of today, the effects of such physical attacks could spread far beyond the radius of a bomb blast. Adding to our physical vulnerability is the fact that information readily available on the World Wide Web (WWW) may disclose to a terrorist the best place to set explosive charges for maximum disruptive effects.

Our dependence on the information and communications infrastructure has created new cyber vulnerabilities, which we are only starting to understand. In addition to the disruption of information and communications, we also face the possibility that someone will be able to actually mount an attack against other infrastructures by exploiting their dependence on computers and telecommunications (see Figure 1).

Physical means to exploit physical vulnerabilities probably remain the most worrisome threat to our infrastructures *today*. But almost every group we met voiced concerns about the new cyber vulnerabilities and threats. They emphasized the importance of developing approaches to protecting our infrastructures against cyber threats ***before*** they materialize and produce major system damage.

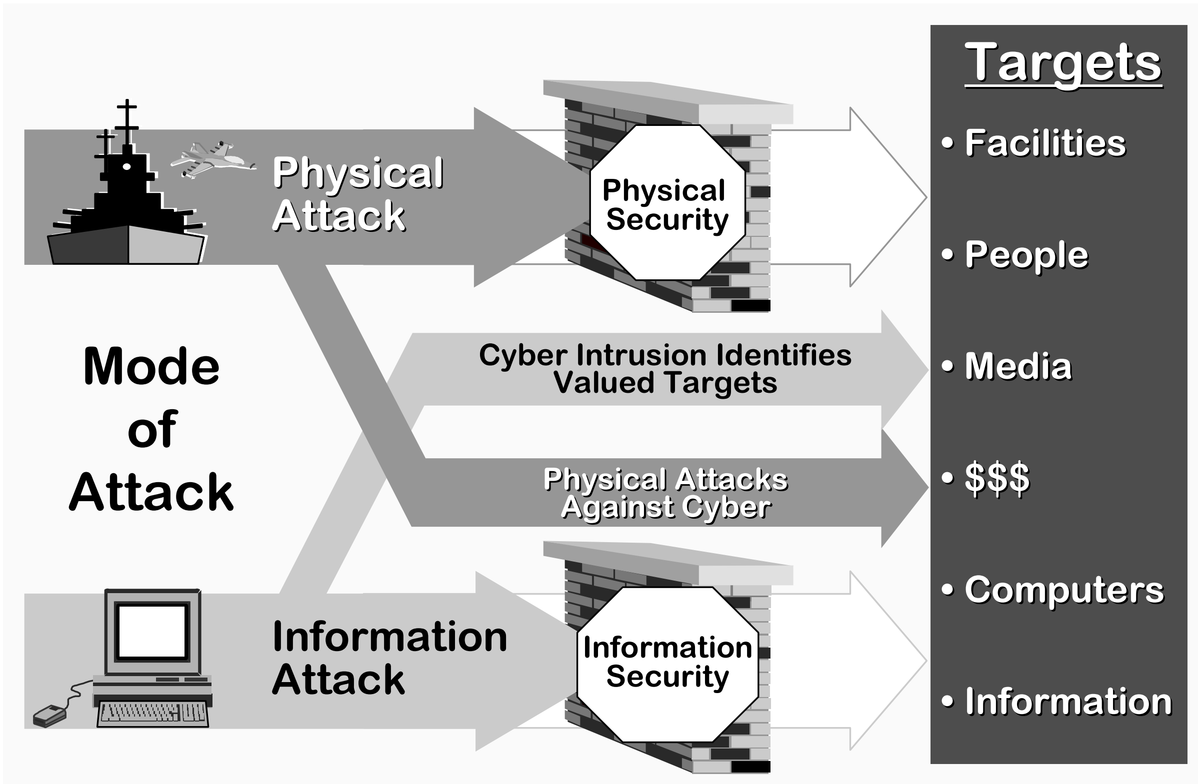

Figure 1. Interdependencies: New Risks and Vulnerabilities

We know our infrastructures have substantial vulnerabilities to domestic and international threats. Some have been exploited—so far chiefly by insiders. Protecting our infrastructures into the 21st Century requires that we develop greater understanding of their vulnerabilities and act decisively to reduce them. It was for just this purpose that President Clinton called into being the President's Commission on Critical Infrastructure Protection in July 1996. In the fifteen months since its creation, the Commission—drawn from the federal government and the private sector—has thoroughly reviewed the vulnerabilities and threats facing our infrastructures, assessed the risks, consulted with thousands of experts, and deliberated at length as to how best to assure our nation's critical foundations in the decades to come. Our analyses, findings, conclusions, and recommendations form the substance of this report.

Our fundamental conclusion is this:

Waiting for disaster is a dangerous strategy. Now is the time to act to protect our future.

Chapter Two

The New Geography

"As borders open and the flow of information, technology, money, trade, and people across borders increases, the line between domestic and foreign policy continues to blur."

— President William J. Clinton, "A National Security Strategy for a New Century," May 1997

Few enemies of the United States have ever had the means to seriously threaten our heartland. Even in the darkest early days of World War II, just after Pearl Harbor, no enemy had the shipping, landing craft, or forces to invade the continental US, or aircraft with the range to reach the mainland and return. For most of our history we've never had to worry much about being attacked at home; broad oceans east and west and peaceable neighbors north and south gave us all the protection we needed.

In the early 1950s, the geography that kept us safe was overcome by Soviet long-range bombers and intercontinental ballistic missiles aimed not only at our military capabilities, but also at the industries and institutions that give our nation its character. We had to learn to think differently about our safety and security. We built backyard bomb shelters, and whole generations of us practiced diving beneath our school desks at the sound of a siren. Our fear of surprise nuclear attack slowly faded as we developed satellites and other early warning capabilities that enabled us to overcome geography and detect a Soviet missile launch in time to launch our own missiles—thus ensuring the credibility of the deterrent policy of Mutual Assured Destruction.

The demise of the Soviet Union, "detargeting" of nuclear missiles, and strategic arms reductions appear to have left America once more relatively invulnerable to physical attack by foreign nations. However, as the threat of a nuclear war has diminished, new technologies have appeared that render physical geography less relevant and our domestic sanctuary less secure. Today, a computer can cause switches or valves to open and close, move funds from one account to another, or convey a military order almost as quickly over thousands of miles as it can from next door, and just as easily from a terrorist hideout as from an office cubicle or military command center. A computer message from Earth can steer a vehicle and point a camera on the surface of Mars. A false or malicious computer message can traverse multiple national borders, leaping from jurisdiction to jurisdiction to avoid identification, complicate lawful pursuit, or escape retribution.

Vulnerability to an adversary using cyber tools was examined during a military exercise[1] conducted in early summer of 1997. The scenario featured “scripted” attacks on the energy and telecommunications infrastructures (controllers injected incidents into the scenario; military commands and government agencies reacted as though the reported incidents were real). Companies providing electrical power in selected cities were subjected to scripted attack by cyber means, over time, in a way that made the resulting simulated outages appear to be random and unrelated. Concurrently, a “Red Team” used hacker techniques available on the Internet to attempt to penetrate Department of Defense (DoD) computers. With no insider information, and constrained by US law, the team spent three months probing the vulnerabilities of several hundred unclassified computer networks. They were able to penetrate many of these networks, and even gained system administrator level privileges in some.

Simulated cyber attacks on nearby privately owned energy companies and telecommunications service providers and successful penetrations into DoD computers were assessed by controllers as sufficient to have disrupted operations at selected military bases—creating a situation in which our ability to deploy and sustain military forces was degraded. Was this exercise an overstatement of today’s vulnerabilities or a glimpse at future forms of terrorism and war? The experience to date, the known vulnerabilities, and the continuing pace of change suggest the latter.

In short, the day may be coming when an enemy can attack us from a distance, using cyber tools, without first confronting our military power and with a good chance of going undetected. The new geography is a borderless cyber geography whose major topographical features are technology and change.

But it is also a global geography. The world’s economy is integrated as never before. With rapid movement of capital, labor, goods and services, technology, and above all, information, across frontiers, our businesses have global outlooks, customers, and needs. In this global economy, communications give even small nations equal access to markets. A nation may no longer need to control territory to have access to its resources.

These changes also have a dark side. As a result of global economic integration, made possible in large measure by information technology, operations of US infrastructures extend far beyond our national boundaries, and even beyond our control. As networks extend to new markets and new sources, new points of entry are established, providing conduits of attack to adversaries at home and abroad. International terrorism, narcotics trafficking, and transnational economic crime are also features—undesirable features—of the new geography.

[1] Chairman of the Joint Chiefs of Staff Exercise ELIGIBLE RECEIVER 1997.

Technology and Change

Fifteen years ago, there were few cell phones or computers and Internet access was limited. The World Wide Web did not exist, nor did today's widely used e-mail systems.

Today, in the United States alone, there are about 180 million computers. Worldwide, there are some 1.3 million local area networks. Computers communicate regionally, nationally, and globally across thousands of wide area networks or through the Internet.

The pace of technological change and our reliance on technology are suggested in Table 1, which compares worldwide populations of 1982 with those of a year ago and those projected to exist in 2002.[2] This table illustrates the growth in the number of potential targets for a cyber attack. It also shows the growth in the number of people having the technical skills necessary to launch such an attack. Of particular significance is the fact that in the past 15 years, the public telecommunications network has become increasingly software driven, remotely managed and maintained through computer networks. The last line of the table shows the population of systems control software specialists who possess the tools and know-how to disrupt or take down the public telecommunications network.

Table 1. Global Technology Trends

Category	15 Years Ago	1996	5 Years Hence
Personal Computers	Thousands	400 million	500 million
Local Area Networks	Thousands	1.3 million	2.5 million
Wide Area Networks	Hundreds	Thousands	Tens of thousands
Viruses	Some	Thousands	Tens of thousands
Internet Devices Accessing the World-Wide Web (WWW)	None	32 million	300 million
Population With Skills for a Cyber Attack	Thousands	17 million	19 million
Telecommunications Systems Control Software Specialists	Few	1.1 million	1.3 million

[2] Technical population data, programmers and telecommunications, 1982-2025, International Data Corporation, and e-mail and documents from the National Computer Security Center, National Security Agency, July 29, 1997.

Effects of the New Geography on Infrastructures

Profound change within the global marketplace, interdependency, restructuring, and reliance on technology make protection a continuing challenge for business and national leaders. The ever-expanding global information infrastructure underpins the global economy. Both business and government must adjust to a borderless world of unrestricted transactions and communications.

Many major infrastructure industries, particularly telecommunications and electricity, are being affected by deregulation and are restructuring to compete at home and in the global marketplace. Organizations have harnessed information technology to accelerate their delivery of goods and services, tighten the efficiency of their processes, and shed excess inventory and unused reserve capacity. Many businesses are so tightly balanced in their “just-in-time” processes that recovery from even a minor disruption would prove difficult.

In sum, technology and change produce better service at lower cost, new markets and more efficient processes throughout the nation and indeed the world. As a result, we depend more than ever on infrastructure services. But at the same time, market forces result in a diffusion of accountability, a decrease in “end-to-end” or system-wide analysis and responsibility, less research and development investment, and a reduction in reserve capacity. Today’s processes are more efficient, but they lack the redundant characteristics that gave their predecessors more resilience.

All of us—government and business, service providers, and service consumers—must pay attention to, and think differently about, a new geography that is global in the physical dimension and without borders in the cyber dimension.

Chapter Three

New Vulnerabilities, Shared Threats, Shared Responsibility

"We face no imminent threat, but we do have an enemy—the enemy of our time is inaction."

— President William J. Clinton, State of the Union Address, January 1997

New Vulnerabilities

Each of the infrastructures is vulnerable in varying degrees to natural disasters, component failures, human negligence, and willful human misconduct. The Commission divided its work into five "sectors" based on the common characteristics of the included industries, and found a mix of physical vulnerabilities, many first identified in the 1980s, and newer cyber vulnerabilities. Results of the sector team studies are in Appendix A. Key points are summarized below.

Information and Communications

All critical infrastructures are increasingly dependent on information and communications. The most important impact and vulnerability for this sector is the increasing interdependency of the PTN and the Internet. The Internet depends heavily on the PTN. The PTN, in turn, depends on electrical power for operations and on telephone lines and fiber optic cables that often run along transportation routes. The PTN is increasingly software driven, and remotely managed and maintained through computer networks. Deregulation of the telecommunications industry will markedly increase the number of access points, increasing opportunities for attack.

One well-publicized example of vulnerability associated with our dependence on computers is the "Year 2000" problem, which, if not corrected, has the potential to adversely affect the operations of all our infrastructures. Solving the Year 2000 problem was not part of the Commission's mission, and efforts are under way elsewhere in the federal government and across the country to remedy the problem before computer clocks turn to 00. But within the bounds of our mission, we did observe that resolving the Year 2000 problem requires the complete review and possibly the substantial revision of an affected organization's operational computer programs. Many people will have to be given access to these programs, as well as the authority to modify them and place them in service with less than adequate testing. The vulnerability will be worse if, as we expect, much of the review and modification work is contracted to outside, perhaps even foreign, firms. An adversary with access to a company's operational computer programs could understand aspects of the company's business practices better than the company's own management, which in turn would allow that adversary to design a subtle or comprehensive attack to gather information or reduce system effectiveness.

Energy

Prolonged disruption in the flow of energy would seriously affect every infrastructure.

The significant physical vulnerabilities for electric power are related to substations, generation facilities, and transmission lines. Large oil refineries are also attractive targets. The increase in transportation of oil via pipelines over the last decade provides a huge, attractive, and largely unprotected target array. Oil and gas vulnerabilities include lines at river crossings; interconnects; valves, pumps, and compressors; and natural gas city gates. Large metropolitan areas could be deprived of critical fuel for an extended period by a properly executed attack.

The widespread and increasing use of Supervisory Control and Data Acquisition (SCADA) systems for control of energy systems provides increasing ability to cause serious damage and disruption by cyber means. The exponential growth of information system networks that interconnect the business, administrative, and operational systems contributes to system vulnerability.

Banking and Finance

The principal vulnerabilities of the banking and finance sector are physical in nature. Its payments systems and its securities and commodities exchanges with their clearing and settlement organizations are vital to other parts of the banking and financial system and the economy at large. There are few of them, and in some cases, they are geographically concentrated. To back up its payments systems, the Federal Reserve has three geographically dispersed and "hardened" sites, each capable of completing the full volume of transactions sent over its wire transfer system. Similar back-up and "hardening" of facilities can be found in the other electronic payments and messaging systems, and most exchanges have a variety of contingency arrangements to rechannel trading activities should anyone's facilities become inoperable. In addition, the principal clearing and settlement organizations for the major stock exchanges have back-up sites some distance from the primary sites, as well as cold storage sites for data. These arrangements, together with strong measures to "harden" primary facilities, greatly reduce the overall vulnerabilities of this sector, but there remains risk from any event that disrupts telecommunications service and electric power within the geographic area in which key facilities are concentrated.

Physical Distribution

While the vulnerabilities of the physical distribution sector are still predominantly physical in nature, there are emerging cyber vulnerabilities as the sector increasingly relies on information technology to shorten lead times, route and schedule traffic and more—all on increasingly crowded communications channels. Physically most significant are the bridges over waterways, which are crossed by personal and commercial transportation, railroad tracks, telecommunications cables, and gas and oil pipelines. Vulnerabilities of the information and communications infrastructure also affect every aspect of the transportation industry. The most significant projected vulnerabilities are those associated with the modernization of the National Airspace System (NAS) and the plan to adopt the Global Positioning System (GPS) as the sole basis for radionavigation in the US by 2010.

Vital Human Services

Emergency responders are inadequately trained and equipped to respond to a chemical, biological, or nuclear attack on a civilian target. The 911 system can be overloaded through misuse and mischief, thereby missing life-and-death calls. Response coordination is vulnerable because the allocated radio frequencies used for responder communications are becoming congested and inadequate.

Treated water supplies do not have adequate physical protection to mitigate the threat of chemical or biological contamination, nor is there technology available to allow the detection, identification, measurement, and treatment of highly toxic, waterborne contaminants. Cyber vulnerabilities include the increasing reliance on SCADA systems for control of the flow and pressure of water supplies.

Government services are dependent on mega-databases of a highly confidential nature and containing information on private citizens. The uneven security practices of government agencies allow exploitation through the cyber vulnerabilities of these databases.

Shared Threats

A *threat* is traditionally defined as a *capability* linked to hostile *intent.* Linking capability to intent works well when malefactors are clearly discernible and US intelligence agencies can focus collection efforts to determine what capabilities they possess or are trying to acquire. During the Cold War, for example, weapons with potential to threaten the United States took years to develop, involved huge industrial complexes, and were on frequent display in large military exercises. Today, however, malefactors are no longer necessarily nation-states, and expensive weapons of war are joined by means that are easier to acquire, harder to detect, and have legitimate peacetime applications. The tools designed to access, manipulate, and manage the information or communications components that control critical infrastructures can also be used to do harm. They are inexpensive, readily available, and easy to use.

While poor design, accidents and natural disasters may threaten our infrastructures, we focused primarily on hostile attempts to damage, misuse, or otherwise subvert them. The Commission looked at both physical and cyber threats; however, we concentrated on the fundamentally new security challenges presented by networked information systems. Key points are summarized below.

Physical Threats

Physical threats fall into two general categories. The first includes threats posed by explosives, such as the World Trade Center and Oklahoma City bombings. Also included are a number of less well-known attacks and thwarted attacks on facilities like electric power transformers and utility towers over the past decade. A much more significant aspect of this threat exists in the form of nuclear weapons. Reports from Russia suggest that some so-called “suitcase weapons” are unaccounted for and may have fallen into the hands of terrorists. Federal Bureau of Investigation (FBI) Director Louis Freeh recently testified that while there is no hard evidence to confirm these reports, they are being treated with utmost seriousness.[3] Increasing attention is also being focused on chemical, biological and radiological threats. Chemical agents have already been used by terrorists, in the 1995 Aum Shinrikyo gas attack in Tokyo. In addition, work done for the

3 Testimony of FBI Director Louis J. Freeh before the House Committee on International Relations, October 1, 1997.

Commission by a national laboratory found there is a credible threat to the nation's water supply systems from biological and chemical agents.

The second category is electronic weapons designed to attack computer-based systems. Included here are radio-frequency devices that capture computer signals as they emanate from the equipment, and electromagnetic pulse and radio-frequency weapons that are intended to destabilize or destroy sensitive electronic components. We determined that weapons of the latter type are still in exploratory stages.

In examining physical threats, the Commission concentrated on two critical issues:

1) the targeting of key links and nodes whose destruction might ripple through infrastructures or across infrastructures, and
2) coordinated attacks which, in combination, could severely impact the nation's security and economic competitiveness.

Simulation exercises with senior representatives of the infrastructures and government shed some light on potential impacts of such attacks, but much more work is needed to understand the implications of interdependent infrastructures.

Cyber Threats

The Commission focused more on cyber issues than on physical issues, because cyber issues are new and not well understood. We concentrated on understanding the tools required to attack computer systems in order to shut them down or to gain access to steal, destroy, corrupt or manipulate computer data and code. In addition to accidents and negligence, threats to computer systems cover a broad spectrum that ranges from prankish hacking at the low end to organized, synchronized attacks at the high end. But the basic attack tools—computer, modem, telephone, and user-friendly hacker software—are common across the spectrum and widely available.

Potential cyber threats and associated risks range from recreational hackers to terrorists to national teams of information warfare specialists. Repeatedly identified as the most worrisome threat is the *insider*—someone legitimately authorized access to a system or network. Other malefactors may make use of insiders, such as organized crime or a terrorist group suborning a *willing* insider (a disgruntled employee, for example) or making use of an *unwitting* insider (by getting someone authorized network access to insert a disk containing hidden code, for example).

Five examples of new types of attack help illustrate the way commonplace cyber tools can be used to do harm.

A Cyber Attack on the Specific Data Base of an Owner/Operator

In the case of unauthorized entry into a network or system for the purpose of illegal financial transfers, stealing proprietary information, disrupting records, or merely "browsing," owners and operators have a responsibility for prudent and sufficient security systems such as firewalls and passwords and qualified personnel to detect anomalies that indicate a successful entry so that further isolation or deflection measures can be taken to foil the attack.

A Cyber Attack for the Purpose of Gaining Access to a Network

If a particular system or network is discovered through "electronic reconnaissance" to have low security standards and to be interconnected to other networks of interest to the attacker, the attacker will use the most weakly defended pathway for access to the targeted system. This suggests that owners and operators need to consider establishing security standards for those with whom they are connected.

A Cyber Attack for the Purpose of Espionage

Intellectual property is vulnerable to theft in entirely new ways. The threat may come from a witting or unwitting insider, an unscrupulous competitor, or the intelligence service of a foreign power. Competitive advantage may be lost without knowing it was even at risk. This is true in business as well as in government.

A Cyber Attack for the Purpose of Shutting Down Service

Attacks by flooding communication lines have denied 911 service in some communities and shut down e-mail service to major users. Denial-of-service attacks are of concern to all institutions whose business depends on reliable communications. Sharing information about the tools used in these attacks and techniques to deflect or defeat them is therefore of interest to a wide range of public and private institutions.

A Cyber Attack for the Purpose of Introducing Harmful Instructions

An attacker can plant a virus or leave behind a program that will give the attacker critical information, such as passwords that can be used to log in to other networks. A virus may be transmitted within a local area network or passed on to an external net. "Logic Bombs" and "Trojan Horses" are designed, respectively, to destroy software at a preselected time and to enable future access. Given the rate of development of viruses, it is essential that all interconnected users adopt a high level of virus detection.

The Internet

Threats to the Internet are of primary concern because we are becoming increasingly dependent on it for communications—including government and military communications—for commerce, for remote control and monitoring of systems, and for a host of other uses; because our ability to understand its full impact on society seems unable thus far to keep up with its explosive growth; and because it is inherently insecure (see Figure 2).

The Internet was designed in 1968 by the then Advanced Research Projects Agency (ARPA), now the Defense Advanced Research Projects Agency (DARPA), to determine how to build resilient computer networks that could survive physical attacks or malfunctions in portions of the network. The ARPAnet, as it was called, was not designed as a secure network, but depended for security on a small number of users who generally knew and trusted one another.

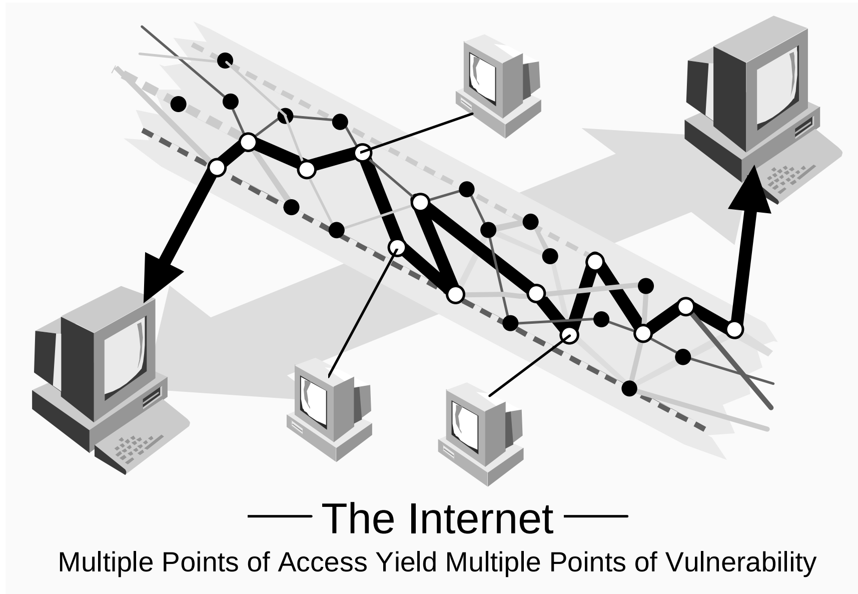

Figure 2. Increasing Exposure

Commercialization of the Internet in the early 1990s, boosted by the WWW, caused incredible growth. Government and the private sector began to seize the advantages of the Internet as an alternative to other unclassified means of communication. The Internet continues to proliferate globally. In general our growing proclivity to network continues to outpace network protection. The price for the efficiency of networking is increased exposure of data and systems to unauthorized and anonymous access. A study done for the Commission by Carnegie-Mellon University's Computer Emergency Response Team (CERT) confirmed that "because the ties between critical infrastructures and the Internet will continue to become stronger and more intricate, the impact of an Internet attack could be devastating."[4]

Information Warfare

Even more recent than the evolution of the Internet has been development and open discussion of the concept of Information Warfare (IW). The Gulf War illustrated the importance of infrastructures to national defense—our domination of Iraq's information and communications ensured victory over a well-armed military force with minimum allied losses. Other nations have drawn similar conclusions. Offensive IW, in brief, uses computer intrusion techniques and other capabilities against an adversary's information-based infrastructures. The Commission is aware of little in the way of special equipment required to launch IW attacks on our computer systems; the basic attack tools—computer, modem, telephone, and software—are essentially the same as those used by hackers and criminals. And compared to the military forces and weapons that in the past threatened our infrastructures, IW tools are cheap and readily available (see Figure 3).

If the basic cyber attack tools and skills are common across the spectrum, what may distinguish recreational hackers from Information Warriors is ***organization***. Said another way,

4 CERT report to the Commission, January 1997, p. 3.

an IW attack against US infrastructures may be little more than a series of hacker attacks, conducted against carefully chosen and thoroughly reconnoitered targets, synchronized in time, to accomplish specific purposes.

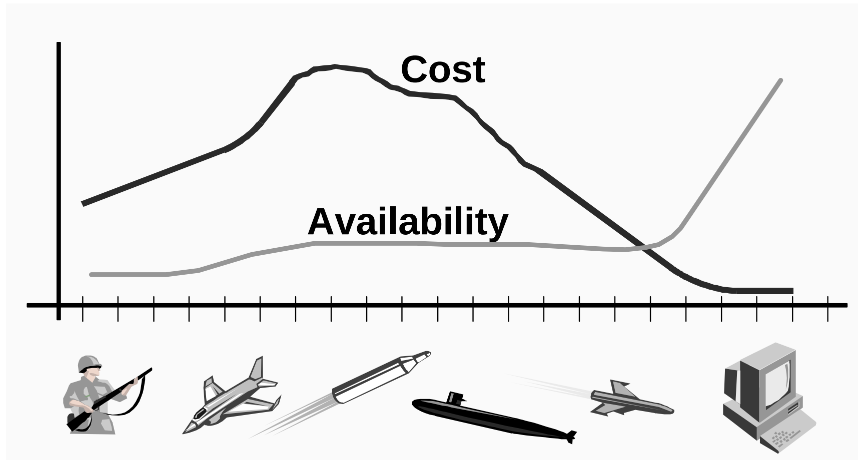

Figure 3. Tools to Do Harm

For an adversary willing to take greater risks, cyber attacks could be combined with physical attacks, against facilities or against human targets, in an effort to paralyze or panic large segments of society, damage our capability to respond to incidents (by disabling the 911 system or emergency communications, for example), hamper our ability to deploy conventional military forces, and otherwise limit the freedom of action of our national leadership.

Terrorists frequently choose prominent targets that produce little physical impact beyond the target itself, but widespread psychological impact. For a physical attack on infrastructures, less spectacular targets could be chosen, such as switching stations, communications antennas, pipelines, transformers, pumping stations, and underground cables. Many facilities whose physical damage or destruction would have a disruptive effect on an infrastructure are purposely located in sparsely populated or even unpopulated areas. If they are physically attacked it may take some time to discover the nature of the damage, and in the absence of casualties it may be some time before the attacks are reported. Even when they are reported, each incident is at first a local event, and if several such events occur over a period of weeks or months it may take considerable time before they are recognized as part of a pattern. Recognition that an attack is in progress could be delayed even if physical attacks were to occur simultaneously, if the targets were spread across several jurisdictions and no mass casualties were produced to generate "breaking news" at the national level.

The chances of immediately discovering that a concerted cyber attack is in progress are today even slimmer. Computer intrusions do not announce their presence the way a bomb does. Depending on the skill of the intruder and the technology and training available to their own system administrators, individual companies whose networks are penetrated may or may not detect an intrusion. Intrusions that are discovered may or may not be reported to law enforcement authorities, who may or may not have the resources to investigate them and conclude whether they are the work of an insider, a hacker, a criminal, or someone truly bent on harming the infrastructure. It sometimes takes months, even years, to determine the significance of individual computer attacks. In the highly publicized 1994 Rome Labs case, the main intruder—a London teenager—was caught in the act; but his alleged accomplice and mentor—who turned out to be a

Welsh computer specialist only a couple of years older—was not identified and arrested until more than two years later.

In the absence of intrusion detection tools, uniform reporting of incidents as they occur, and some central capability to analyze incidents as they are reported, it is conceivable that an orchestrated attack against US infrastructures could be under way for some time before it is recognized as such and the attacker's motives and objectives can be deduced.

Intelligence Community Challenges

Information Warfare presents significantly new challenges for the intelligence community in identifying and assessing threats to the United States. This is partly because concepts of IW are only now taking shape abroad and because tools and techniques used for IW attack are inexpensive and ubiquitous. It is clear that a number of nation-states are closely following US developments in IW and are themselves exploring IW capabilities. They recognize that modern industrialized states are increasingly dependent on the uninterrupted flow of information. In addition, sub-national groups increasingly rely on advanced information technologies to support their illegal operations, and US intelligence analysts must be on the look-out for indications of interest by these groups in using their technical knowledge to harm the United States by attacking our critical infrastructures.

Recent assessments of foreign IW threats suggest a measured apprehension about the future. While no one is forecasting a sudden and major IW attack on the United States in the next few years, a number of factors support the sense of a growing threat. The US is by no means alone in recognizing and seizing the advantages of the global information and communications infrastructure and thus the increasing likelihood of various forms of international competition in the information arena. It is reasonable to assume that the number of states following our lead will increase. Other states and non-state groups will become increasingly familiar with opportunities for offensive use of computer techniques as they develop their own technology base and necessary cyber defensive capabilities. Finally, computer crime, including that directed against American businesses, will continue to grow in nation-states that do not enforce strong prosecution.

Shared Responsibility

The government and private sector share substantially the same national information infrastructure. Both have been victims of unauthorized computer intrusions, theft, and disruption. In our view, the line separating threats that apply only to the private sector from those associated with traditional national security concerns must give way to a concept of shared threats (see Figure 4). Shared threats demands a shared response, built from increased partnership between government and the owners and operators of our infrastructures.

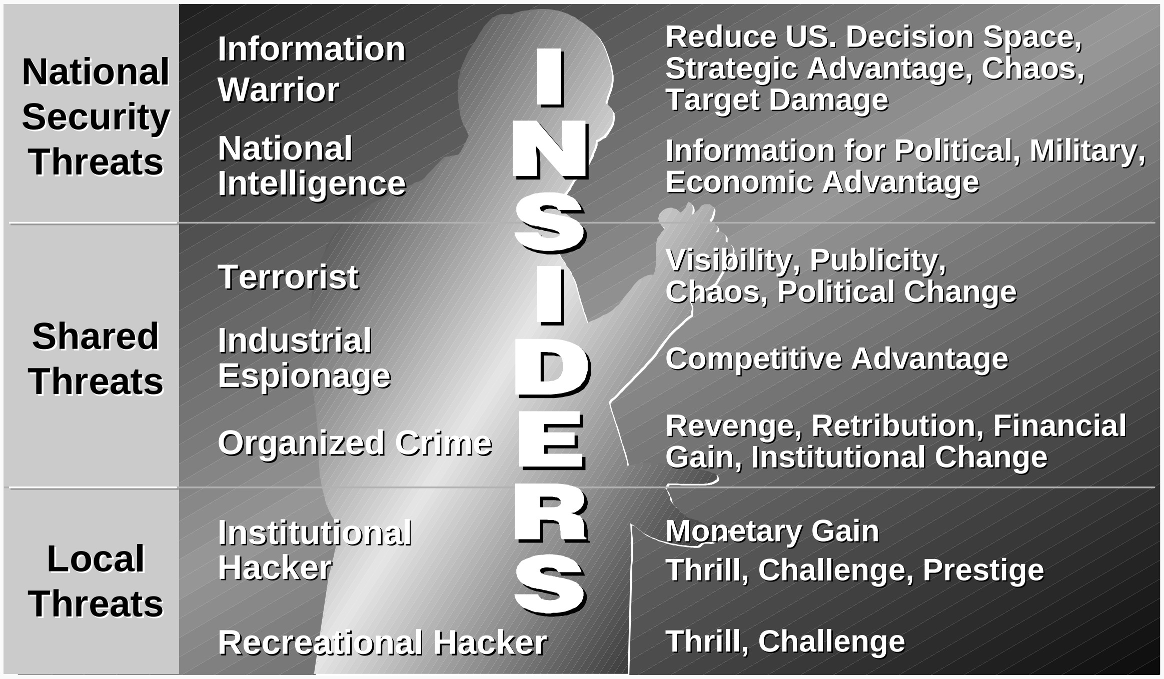

Figure 4. Threat Spectrum

Factory owners or service providers were not expected in the past to protect themselves from enemy bombers or missiles; that was government's job. In the future, though, the owners and operators may be on the front line, and their networks may be the battlefield. The tools and know-how required to do harm are inexpensive, readily available, and easy to use.

Owners and operators need to protect themselves from the tools and the know-how. Government can help by collecting and disseminating information about all the tools that can do harm. Owners and operators can help by informing government when new tools or techniques are detected. Government has an obligation to collect information about potentially hostile groups and nation-states, and to issue timely warnings alerting owners and operators when new threats are detected.

We must achieve a new understanding of the threats that confront us—an understanding that focuses on the capability to do harm rather than identifying the person, group or nation intent on doing harm. Traditional indicators of developing capability are not present. There are no missile silos to count or railway cars to examine. We must acknowledge that the capacity for harm exists, and act now, as partners, to protect our future.

Chapter Four

Findings and Policy

Analysis of the infrastructures, their vulnerabilities, and shared threats led the Commission to several observations. This chapter sets out those findings and then suggests a policy framework that addresses them. Subsequent chapters deal with specific recommendations resulting from that process.

In some respects our most important finding was the need to think differently about infrastructure protection. The management approach we now use was designed to deal with the Industrial Revolution, then was adjusted to manage successively the stabilization of America after the Civil War, the Depression, World War II, and finally the nuclear stand-off of the Cold War. None of those approaches is particularly applicable to the world as it will look through the lens of information technology in the third millennium.

FINDING: Information sharing is the most immediate need.

There are many instances in which information is shared between the private sector and government, as in the case of the North American Electric Reliability Council (NERC) and the Presidentially-appointed National Security Telecommunications Advisory Committee (NSTAC). But there are important shortfalls. Increasing the sharing of strategic information within each infrastructure, across different sectors, and between sectors and the government will greatly assist efforts of owners and operators to identify their vulnerabilities and acquire tools needed for protection.

FINDING: Responsibility is shared among owners and operators and the government.[5]

[5] While sometimes these owners and operators are referred to as the "private sector," in truth the infrastructures also include publicly-owned and operated activities such as municipal water companies, state and local highway departments, and fire, police, and emergency response agencies.

Owners and operators have always focused on protecting themselves from known threats to their operations, because it is in their interest. The government has always focused on protecting the nation from threats beyond the capabilities of private self-protection. Today, an adversary can bypass our national defense forces to attack directly the infrastructures that underpin our national economic strength. Traditional national security concerns must give way to a concept of shared threats, for which responsibility must be shared between government and infrastructure owners and operators.

FINDING: **Infrastructure protection requires integrated capabilities of diverse federal agencies, and special means for coordinating federal response to ensure these capabilities are melded together effectively.**

The Commission believes that the federal government's job in infrastructure protection includes the traditional defense, law enforcement, intelligence, and other responsibilities as well as the additional effort, resources and processes to respond to the cyber dimension. The structures detailed in our recommendations are designed to expand the reach of existing capabilities, provide a means to coordinate them, and integrate them with the resources of the owners and operators.

FINDING: **The challenge is one of adapting to a changing culture.**

Our culture is changing at an accelerating pace. The Information Age is still unfolding, but it is already clear that it brings with it at least as many adjustments to our way of life as did the Industrial or the Nuclear Age, and that the requirement to adapt will be more urgent. Bold, sweeping measures are required to educate and inform our private sector, public servants, and citizens about the realities of the new environment.

FINDING: **The federal government has important roles in the new infrastructure protection alliance with industry and state and local governments.**

The federal government is in a position to lead by example by adopting best practices, actively managing risk, and improving security planning in its own systems.

FINDING: The existing legal framework is imperfectly attuned to deal with cyber threats.

Laws change at a much slower rate than technology. The existing legal framework does not reflect current technology in a number of ways. Legal authorities will need to be modified to allow for greater awareness of information security concerns, to enable response to and recovery from cyber events, to increase deterrence against computer crimes domestically and internationally, and to clarify roles and responsibilities in a world that is increasingly moving away from jurisdictional boundaries.

FINDING: Research and development are not presently adequate to support infrastructure protection.

New challenges require new resources and new examination of how to protect ourselves. The Commission's proposed research and development (R&D) program identifies specific areas for research to provide the needed technologies.

Toward Recommendations

As we approached making recommendations to assure our critical infrastructures, the Commission adopted a set of principles to guide our decisions.

- ***Build on that which exists.*** It will be easier and faster to implement, more effective, and more likely to be accepted than creating something new.
- ***Depend on voluntary cooperation***. Partnerships between industry and government will be more effective and efficient than legislation or regulation.
- ***Start with the owners and operators***. They have a strong economic stake in protecting their assets and maximizing customer satisfaction. They understand the infrastructures and have experience in responding to outages.
- ***Practice continuous improvement***. Take action in affordable increments. There is no "magic bullet" solution. Aim not only to protect the infrastructures, but also to enhance them.
- ***Coordinate security with maintenance and upgrades***. Security should be incorporated in planned maintenance and scheduled upgrades.
- ***Promote government leadership by example.*** Government-owned facilities should be among the first to adopt best practices, active risk management, and improved security planning.
- ***Minimize changes to government oversight and regulation***. Several of the infrastructures have a long history of government regulation, with a clear legislative mandate and a record of success. We consciously avoided proposing significant changes in regulation.

A Proposed National Policy for Infrastructure Protection

Critical infrastructures underpin the security of our national wealth, our defense capability, the economic prosperity of the people, and, above all, the maintenance of the system of human rights and individual freedoms for which the United States was founded and has stood since 1776. The threat of infrastructure attacks therefore has the potential for strategic damage to the United States. Accordingly, the assurance of critical infrastructures deserves national attention and leadership by the federal government.

It shall be the policy of the US to assure the availability and continuity of the critical infrastructures on which our economic security, defense, and standard of living depend. The infrastructures will be defended by whatever means necessary, including the full range of business, legal, law enforcement, military, and social tools available.

Further, the US recognizes that assuring infrastructure is not just a government or business responsibility, but is shared by those public and private interests that own and operate the infrastructures and the government agencies responsible for defense, law enforcement, and economic security of the nation.

The interdependent nature of the critical infrastructures and their collective dependence on the information and communications infrastructure have created new assurance challenges that can only be met by a partnership between owners and operators and government at all levels. Only the owners and operators have the knowledge, access, and technology to defend their systems from the growing array of widely available information-based tools. Only the federal government has the legal authority, law enforcement capability, and defense and intelligence resources needed to deter the most sophisticated nation-state and other serious cyber threats. And only the federal government has the intelligence and related capabilities to find the tools that do harm and promulgate information about them throughout the infrastructures.

As a matter of urgency, an Office of National Infrastructure Assurance should be established under the National Security Council (NSC) and given overall program responsibility for infrastructure assurance matters, including policy implementation, strategy development, federal interagency coordination, and liaison with state and local governments and the private sector. Among other responsibilities, this Office will devise and establish mechanisms for the exchange of views and information between the government and the private sector, identify information requirements for infrastructure assurance, and ensure that infrastructure assurance considerations are taken into account in making other government program decisions.

The Office of National Infrastructure Assurance should ensure that a program of public awareness is implemented throughout the country to inform the American public about infrastructure protection. This will include establishment of appropriate curricula in the national education system, from kindergarten through graduate school and including professional training. The Office of National Infrastructure Assurance should also ensure that individual agencies of the federal government implement infrastructure preparedness provisions and update their security plans to include protection against Information Warfare threats.